
FEDERAL TRADE COMMISSION DECISIONS

FINDINGS, OPINIONS, AND ORDERS
JULY 1, 2008, TO DECEMBER 31, 2008

IN THE MATTER OF

REED ELSEVIER INC.
AND
SEISINT, INC.

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4226; File No. 052 3094
Complaint, July 29, 2008 – Decision, July 29, 2008

This consent order applies to practices of Reed Elsevier Inc. and Seisint, Inc., that failed to provide reasonable and appropriate security for sensitive consumer information stored in Seisint databases. Breaches of the system by identity thieves disclosed sensitive information about more than 300,000 consumers. The order requires each respondent to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of nonpublic personal information collected from or about consumers. The security programs must contain administrative, technical, and physical safeguards appropriate to the respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. The order requires each respondent to obtain on a biennial basis for a period of 20 years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that it has in place a security program that provides protections that meet or exceed the protections required by the order. and its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. The order requires the respondents to retain documents relating to their compliance with the order, to disseminate the order to persons with responsibilities relating to the subject matter of the order, to notify the Commission of changes in corporate status, and to submit periodic compliance reports.

Participants

For the Commission: Katrina A. Blodgett, Kathleen L. Claffie,
Kathryn D. Ratté, Jessica Rich, Alain Sheer, and Joel Winston.

Complaint

For the *Respondents: J. Howard Beales, III; Jeffrey I. Cox, Thomas R. Kraemer, and Ronald I Raether, Faruki, Ireland, & Cox P.L.L.*; and *Emilio W. Cividanes and Lisa Jose Fales, Venable LLP.*

COMPLAINT

The Federal Trade Commission, having reason to believe that Reed Elsevier Inc. and Seisint, Inc. have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Reed Elsevier Inc. (“REI”) is a Massachusetts corporation with its principal office or place of business at 125 Park Avenue, Suite 2300, New York, New York 10017. REI engaged in the acts and practices at issue in this complaint through LexisNexis, a division of REI with its principal office or place of business at 9333 Springboro Pike, Dayton, Ohio 45401.

2. Respondent Seisint, Inc. (“Seisint”) is a Florida corporation with its principal office or place of business at 6601 Park of Commerce Boulevard, Boca Raton, Florida 33487.

3. Respondent REI acquired respondent Seisint on September 1, 2004, and since then has operated it as a wholly-owned subsidiary within LexisNexis. Respondent REI integrated respondent Seisint into LexisNexis by, among other things, using respondent Seisint’s facilities, personnel, technologies, and products in LexisNexis’ other business operations. Since the acquisition, respondent REI has controlled the acts and practices of respondent Seisint at issue in this complaint. Respondent Seisint is solely liable for its practices prior to the acquisition.

4. The acts and practices of respondents as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

Complaint

RESPONDENTS' BUSINESS PRACTICES

5. At all relevant times before and after the acquisition, respondents Seisint and REI have been in the business of collecting, maintaining, and selling information about consumers. Among other things, each respondent sells products that customers use to locate assets and people, authenticate identities, and verify credentials (collectively, "verification products").

6. Respondent Seisint sells verification products under its Accurint trade name (collectively, "Accurint verification products"). Accurint verification product customers include insurance companies, debt collectors, employers, landlords, law firms, and law enforcement and other government agencies. Respondent REI sells similar verification products, under various LexisNexis trade names.

7. In connection with their verification products, respondents:

(a) collect and aggregate information about millions of consumers and businesses from public and nonpublic sources, including motor vehicle records and consumer identification information from credit reporting agencies, and maintain and store the information in computer databases.

(b) operate computer networks and websites and provide software (such as web applications and search engines) through which a customer can use a verification product to search electronically for information in the respondent's computer databases. To conduct such a search, the customer enters a search term, such as a consumer's name, and retrieves through the search other items of information about the consumer.

Complaint

(c) charge customers a fee to search for and retrieve information from their databases.

8. Respondents' databases contain nonpublic and often highly sensitive personal information about consumers, including consumer identification information obtained from credit reporting agencies, such as Social Security numbers. It is widely recognized that misuse of such information – and in particular consumers' Social Security numbers – can facilitate identity theft and related consumer harms.

9. At all relevant times, respondents have implemented procedures to identify customers seeking access to their databases, limit access to nonpublic information to customers meeting certain criteria, and track searches their customers make. Such procedures include:

(a) steps to authenticate customers (or verify that the customers are who they claim to be) before permitting them to search the databases, usually by requiring each customer to log-in using a user ID and a password (collectively, "user credentials").

(b) rules governing the format of user credentials that customers must present for authentication.

(c) rules governing which customers can access nonpublic information and which are restricted to public information only.

(d) codes, assigned to each customer's user credentials, that permit the customer to access the types of information the customer is authorized to access.

Under these procedures, an unauthorized person logging-in with the user credentials of a legitimate verification product customer would be authenticated and could then access all of the

Complaint

information the legitimate customer could access, including sensitive nonpublic information if the customer were so authorized.

RESPONDENTS' SECURITY PRACTICES

10. Until at least mid-2005, respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to the sensitive consumer information stored in databases accessible using Accurant verification products ("Accurant databases"). In particular, respondents failed to establish or implement reasonable policies and procedures governing the creation and authentication of user credentials for authorized customers accessing Accurant databases. Among other things, respondents:

(a) failed to establish or enforce rules sufficient to make user credentials hard to guess. For example, respondents allowed Accurant customers to use the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;

(b) permitted the sharing of user credentials among a customer's multiple users, thus reducing likely detection of, and accountability for, unauthorized searches;

(c) failed to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive nonpublic information;

(d) failed to suspend user credentials after a certain number of unsuccessful log-in attempts;

(e) allowed customers to store their user credentials in a vulnerable format in cookies on their computers;

Complaint

(f) failed to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and respondents' websites;

(g) allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves;

(h) did not adequately assess the vulnerability of the Accurant web application and computer network to commonly known or reasonably foreseeable attacks, such as "Cross-Site Scripting" attacks; and

(i) did not implement simple, low-cost, and readily available defenses to such attacks.

11. By the security practices set out in Paragraph 10, respondents established user ID and password structures that created an unreasonable risk of unauthorized access to sensitive consumer information stored in Accurant databases. Security professionals have issued public warnings about the security risk presented by weak user ID and password structures since the late 1990s, when well-publicized attacks to obtain customer passwords began to occur. Further, from attacks on user ID and password structures controlling access to Accurant databases, respondents have had notice of the risk since at least 2002. In addition, respondents did not use readily-available security measures to prevent or limit such attacks, such as by using well-known procedures that would limit or block attacks on user credentials. As a result of respondents' security practices, an attacker could easily guess or intercept the user credentials of legitimate customers and use them to gain access to sensitive information – including Social Security numbers – about millions of consumers.

Complaint

12. On multiple occasions since January 2003, attackers exploited respondent Seisint's user ID and password structures to obtain without authorization the user credentials of legitimate Accurant customers. The attackers then used these credentials to make thousands of unauthorized searches for consumer information in Accurant databases. These attacks disclosed sensitive information about several hundred thousand consumers, including, in many instances, names, current and prior addresses, dates of birth, and Social Security numbers. Although some of these attacks occurred before respondent REI acquired respondent Seisint, they continued for at least 9 months after the acquisition, during which time respondent Seisint was operating under the control of respondent REI. Since March 2005, respondent REI through LexisNexis has notified over 316,000 consumers that the attacks disclosed sensitive information about them that could be used to conduct identity theft.

13. In a number of the incidents referred to in Paragraph 12, new credit accounts were opened in the names of consumers whose information was disclosed without authorization, and purchases were made on the new accounts. In other instances, identity thieves used sensitive information obtained without authorization from Accurant databases to activate newly-issued credit cards stolen from legitimate cardholders, and then made fraudulent purchases on the cards. In response to such incidents, cards were cancelled and consumers holding them were unable to use them to access their credit and bank accounts until they received replacement cards. Further, because the incidents referred to in Paragraph 12 disclosed Social Security numbers and other sensitive information, several hundred thousand consumers face the possibility of future fraud.

VIOLATIONS OF THE FTC ACT

14. As set forth in Paragraphs 10 through 13, respondents failed to employ reasonable and appropriate measures to prevent

Decision and Order

unauthorized access to sensitive consumer information stored in Accurant databases. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

15. The acts and practices of respondents as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twenty-ninth day of July, 2008, has issued this complaint against respondents.

By the Commission.

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondents named in the caption hereof, and the Respondents having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondents with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondents, their attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the

Decision and Order

Respondents of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondents that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondents have violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Respondent Reed Elsevier Inc. is a Massachusetts corporation with its principal office or place of business at 125 Park Avenue, Suite 2300, New York, New York 10017. Respondent Seisint, Inc. is a Florida corporation with its principal office or place of business at 6601 Park of Commerce Boulevard, Boca Raton, Florida 33487.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, and the proceeding is in the public interest.

Decision and Order

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about a consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals a consumer’s email address; (d) a telephone number; (e) a Social Security number; (f) a date of birth; (g) a driver’s license number; (h) credit and/or debit card information, including but not limited to card number and expiration date and transaction detail data; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies a consumer; or (j) any other information from or about a consumer that is combined with (a) through (i) above.
2. “Information product or service” shall mean each product, service, or other means by which respondents individually or collectively provide direct or indirect access to personal information from or about consumers that is comprised in whole or part of nonpublic information; *provided, however*, that this term shall not include information products or services that: (a) provide access solely to personal information that is publicly available information, or (b) permit customers to upload or otherwise supply, organize, manage, or retrieve information that is under the customer’s control.

Decision and Order

3. “Publicly available information” shall mean information that respondents have a reasonable basis to believe is lawfully made available to the general public from: (a) Federal, State, or local government records, (b) widely distributed media, or (c) disclosures to the general public that are required to be made by Federal, State, or local law. Respondents shall have a reasonable basis to believe information is lawfully made available to the general public if respondents have taken reasonable steps to determine: (a) that the information is of the type that is available to the general public, and (b) whether an individual can direct that the information not be made available to the general public and, if so, that the individual has not done so.
4. “LexisNexis” shall mean Seisint, Inc., and its successors and assigns, officers, agents, representatives, and employees, and the LexisNexis division of respondent Reed Elsevier Inc., and its successors and assigns, officers, agents, representatives, and employees; *provided, however*, that, for the purposes of this order, LexisNexis shall:
 - (a) be treated as a corporation under the control of respondent Reed Elsevier Inc. for the purpose of determining whether any other entity is a successor or assign of LexisNexis; and
 - (b) include any other corporation, subsidiary, division, or other device under the control of respondent Reed Elsevier Inc. (collectively, “entity”) to the extent that such entity advertises, markets, promotes, offers for sale, or sells any information product or service that includes a Social Security number; driver’s license number; date of birth; or bank, credit card, or other financial account number (collectively, “designated information”), including, but not limited to, any

Decision and Order

information product or service that can be used to access, view, or retrieve designated information from databases under the entity's possession or control.

5. Unless otherwise specified, "respondents" shall mean Reed Elsevier Inc., its successors and assigns, officers, agents, representatives, and employees, and Seisint, Inc., and its successors and assigns, officers, agents, representatives, and employees.

I.

IT IS ORDERED that each respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of personal information collected from or about consumers made available through any information product or service of LexisNexis ("the information"), in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of the information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to each respondent's size and complexity, the nature and scope of each respondent's activities, and the sensitivity of the information, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of the information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of the information, and assessment of the

Decision and Order

sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; *provided, however*, that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve, and supply to respondent, additional personal information about the consumer.
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

Decision and Order

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, each respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a

Decision and Order

Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that each respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question its compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Paragraph II of this order: all materials relied upon to prepare the Assessment, whether prepared by or behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments and any other materials relating to its compliance with Paragraphs I and II of this order, for the compliance period covered by such Assessment.

Decision and Order

IV.

IT IS FURTHER ORDERED that each respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Each respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that each respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that each respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file

Decision and Order

with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on July 29, 2028, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Paragraph in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Reed Elsevier Inc. (“REI”) and Seisint, Inc. (“Seisint”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

The Commission’s proposed complaint alleges that REI (through its LexisNexis division) and Seisint are data brokers. REI acquired Seisint on September 1, 2004 and has continued to operate Seisint under the Seisint name; REI also uses Seisint’s technologies and facilities in REI’s LexisNexis data broker business. In connection with Seisint’s business, proposed respondents collect, and store in electronic databases, information about millions of consumers, including names, current and prior addresses, dates of birth, driver’s license numbers, and Social Security numbers (“SSNs”). They also sell products customers use to retrieve information from the databases, including products to locate assets and people, authenticate identities, and verify credentials. Until at least mid-2005, access to information in Seisint databases was controlled using only user IDs and passwords (“credentials”). Seisint customers include insurance companies, debt collectors, employers, landlords, law firms, and law enforcement and other government agencies.

The complaint further alleges that REI and Seisint engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer information stored in Seisint databases. In particular, they: (1)

Analysis to Aid Public Comment

failed to make credentials hard to guess; (2) failed to require periodic changes of credentials (such as every 90 days, for customers with access to sensitive consumer information); (3) failed to suspend credentials after a certain number of unsuccessful log-in attempts; (4) allowed customers to store their credentials in a vulnerable format in cookies on their computers; (5) failed to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and Seisint websites; (6) allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves; (7) permitted users to share credentials; (8) did not adequately assess the vulnerability of Seisint's web application and computer network to commonly known or reasonably foreseeable attacks, such as "Cross-Site Scripting" attacks; and (9) did not implement simple, low-cost, and readily available defenses to such attacks. As a result, an attacker could easily guess or intercept the user credentials of legitimate customers and use them to access sensitive information – including SSNs – about millions of consumers.

The complaint alleges that on multiple occasions since January 2003, identity thieves exploited these vulnerabilities to obtain the credentials of legitimate Seisint customers. The thieves then used the credentials to make thousands of unauthorized searches for consumer information in Seisint databases. These breaches disclosed sensitive information about more than 300,000 consumers, including, in many instances, names, current and prior addresses, dates of birth, and SSNs. In some instances, the thieves opened new credit accounts in the names of consumers whose information was disclosed and made purchases on the new accounts. In other instances, they used the information to activate newly-issued credit cards stolen from legitimate cardholders and then made fraudulent purchases on the cards. Although some of these breaches occurred before REI acquired Seisint on

Analysis to Aid Public Comment

September 1, 2004, they continued for at least 9 months after the acquisition, during which time Seisint was under REI's control.

The proposed order applies to nonpublic information sold by Seisint and LexisNexis, as well as by any other business within REI to the extent that the business sells products that include an SSN, driver's license number; date of birth; or bank, credit card, or other financial account number or information. The order also contains provisions designed to prevent respondents from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires each respondent to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of nonpublic personal information collected from or about consumers. The security programs must contain administrative, technical, and physical safeguards appropriate to the respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires each respondent to:

- Designate an employee or employees to coordinate and be accountable for the information security program.
- Identify material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Analysis to Aid Public Comment

- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from the respondent, and require service providers by contract to implement and maintain appropriate safeguards.
- Evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have material impact on its information security program.

Part II of the proposed order requires each respondent to obtain within 180 days, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires respondents to retain documents relating to their compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, respondents must retain the documents for a period of three years after the date that each assessment is prepared. Part IV requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that each respondent submit a compliance report to the FTC within 180 days, and periodically

Analysis to Aid Public Comment

thereafter as requested. Part VII is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

This is the Commission’s nineteenth case to challenge the failure by a company to implement reasonable information security practices. Each of the Commission’s cases to date has alleged that a number of security practices, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to consumers’ information. The practices challenged in the cases have included, but are not limited to: (1) creating unnecessary risks to sensitive information by storing it on computer networks without a business need to do so; (2) storing sensitive information on networks in a vulnerable format; (3) failing to use readily available security measures to limit access to a computer network through wireless access points on the network; (4) failing to adequately assess the vulnerability of a web application and computer network to commonly known or reasonably foreseeable attacks; (5) failing to implement simple, low-cost, and readily available defenses to such attacks; and (6) failing to use readily available security measures to limit access between computers on a network and between such computers and the Internet. This proposed action against REI and Seisint is the first to challenge alleged security failures involving the security of passwords. Passwords are a critical part of a reasonable and appropriate security program because passwords are typically the first (and are often the only) method used to authenticate (or authorize) users to access resources, such as programs and databases, available on a computer network or online.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.

Complaint

IN THE MATTER OF

THE TJX COMPANIES, INC.CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4227; File No. 072 3055
Complaint, July 29, 2008 – Decision, July 29, 2008

This consent order addresses practices of The TJX Companies, Inc., that failed to provide reasonable and appropriate security for personal information on its computer networks. TJX sells apparel and home fashions in over 2,500 stores worldwide. A breach of its computer networks compromised tens of millions of unique payment cards used by consumers in the United States and Canada. The order requires TJX to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to TJX's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. The order requires that TJX obtain, on a biennial basis for 20 years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that TJX has in place a security program that provides protections that meet or exceed the protections required by the order, and that its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected. TJX is required to retain documents relating to its compliance with the order; to disseminate the order to principals, officers, directors, and managers having responsibilities relating to the subject matter of the order; to notify the Commission of changes in corporate status; and to file compliance reports with the Commission.

Participants

For the *Commission*: *Molly Crawford, Jessica Rich, Alain Sheer, and Joel Winston.*

For the *Respondents*: *Lisa J. Sotto, Hunton & Williams, and Mit Spears, Ropes & Gray LLP.*